LINK11

IN 6 STEPS AND ONE HOUR TO COMPLETE WEB APPLICATION & API PROTECTION

From Backend Definition to Go-Live

In today's digital landscape, web applications and APIs form the gateway to your business. At the same time, they are also a primary target for cybercriminals. However, proactively and comprehensively protecting these critical assets doesn't have to be complex or time-consuming: with the Link11 WAAP platform, an all-in-one solution offering multi-layered protection against DDoS attacks, malicious bots, zero-day exploits, and other threats can be set up easily in just a few steps.

This quick and simple implementation allows IT teams to establish the highest security standards immediately, while saving resources and avoiding lengthy processes.

The Setup Process

1

Definition of the Backend Service

The Foundation of the Connection

First, the data source for the WAAP is determined. It is defined whether communication takes place via domain names or IP addresses, as well as the protocol used (HTTP, HTTPS, or Port Bridge Mode). This ensures the clean routing of traffic to the origin servers.

2

Provisioning the Certificate & Configuring the Load Balancer

Secure SSL Termination

To analyze encrypted traffic, uploading an SSL certificate is required. This can be done by copying and pasting the file or by extracting a PFX file. Crucially, the certificate must then be assigned to the load balancer. Only then can the redundant proxy network consistently perform decryption and inspection across all instances worldwide.

3

Customizing the Security Policy

Individual Rule Set

Copying the „Default Policy“ creates a solid foundation. In this new policy, the application paths are linked to the backend service defined in step 1. Additionally, granular exceptions can be defined here, or critical areas (such as login pages) can be provided with special protection rules.

4

Creating the Server Group

The Logical Bracket

In this step, all components are brought together. A „Server Group“ is created, storing the exact domains or hosts to be protected. This group is linked with the customized Security Policy (from step 3) and the configured certificate (from step 2) to complete the protection profile.

5

Changing the DNS Routing

The Traffic Switch

The visitor traffic is redirected to the protective shield. This requires changing the domain‘s A-record in the DNS management so that it points to the IP address of the Link11 WAAP. From this point on, every request flows through the WAAP‘s filters.

6

Publishing the Configuration

Go Live

Initially, all settings are in a staging environment, which allows for final testing. Only by clicking „Publish“ is the rule set transferred and activated on the global network. As soon as the DNS change has propagated, the infrastructure is fully protected.

Your Benefits at a Glance:
Maximum Protection with Minimum Effort

- **Fast Setup:** Thanks to the intuitive interface and simple processes, the WAAP is fully operational in just one hour. No lengthy integration projects.
- **All-in-One Protection:** Benefit from a powerful combination of Web Application Firewall, Web DDoS Protection, Bot Management, and API Security.
- **Automated Real-Time Defense:** Immediately after setup, your entire data traffic is analyzed in real time to block threats instantly.
- **Resource-Saving Resilience:** Effective protection against downtime, reputational damage, and financial losses with minimal administrative effort, relieving the burden on IT teams.
- **Seamless System Integration:** The WAAP can be effortlessly integrated into existing security structures.

In today's complex and rapidly evolving threat landscape, Link11's Web Application and API Protection (WAAP) platform is a comprehensive solution that protects your most valuable web assets. By integrating a web application firewall, web DDoS protection, robust bot management, and API protection, Link11 offers unparalleled protection with an optimized user experience. Our purpose-built cloud infrastructure, backed by a 100% uptime SLA and GDPR compliance, ensures that your business remains resilient, compliant, and always accessible to legitimate users.

BUILT TO DEFEND. ALWAYS AT YOUR SIDE.

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com